JOSEPH W. PRICE
ALBIN H. GESS
FRANKLIN D. UBELL
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

PRICE, GESS & UBELL
ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com

#2 Priority Paper

PRIORITY DOCUMENT - JAPAN 11-245277

Applicant(s):	Makoto Tatebayashi et al.
Title:	ENCRYPTION METHOD, ENCRYPTION APPARATUS, DECRYPTION METHOD, AND DECRYPTION APPARATUS
Attorney's Docket No.:	NAK1-BM08

"EXPRESS MAIL" MAILING LABEL NO. EL230379070US

DATE OF DEPOSIT: August 15, 2000

J.W. PRICE 949/261.8433
Makoto TATEBAYASHI et al
NAK2-BM08

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

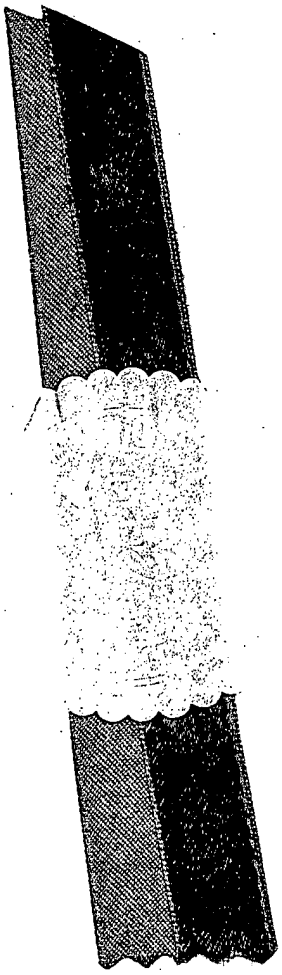
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月３１日

出願番号
Application Number: 平成１１年特許願第２４５２７７号

出願人
Applicant (s): 松下電器産業株式会社
株式会社東芝



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　６月　９日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４３２７６

【書類名】　特許願

【整理番号】　2022510387

【提出日】　平成11年 8月31日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　9/06

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　横田　薫

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大森　基司

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　佐野　文彦

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　遠藤　直樹

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【選任した代理人】

【識別番号】　100109210

【弁理士】

【氏名又は名称】　新居　広守

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9810105

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ暗号化装置及び暗号処理方法

【特許請求の範囲】

【請求項１】　入力データをＮビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを前記初期値に初期化するデータ記憶手段と、

前記データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

前記データ変換手段から出力されたデータと前記鍵データを融合するデータ融合手段と、

前記所定の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第１の部分鍵生成処理を行い、前記所定の入力ブロック以外の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第２の部分鍵生成処理を行う部分鍵生成手段と、

前記部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

前記部分鍵生成手段で行う前記第１の部分鍵生成処理と前記第２の部分鍵生成処理は安全性のための処理負荷を異ならせていることを特徴とするデータ暗号化装置。

【請求項２】　前記第２の部分鍵生成処理は、前記データ融合手段から出力されたデータに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって行い、これにより、前記第１の部分鍵生成手段よりも安全性のための処理負荷を小さくしていることを特徴とする請求項１記載のデータ暗号化装置。

【請求項３】　前記データ融合手段におけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする請求項１記載のデータ暗号

化装置。

【請求項４】　前記所定の入力ブロックは、Ｍ番目毎に入力される入力ブロックであって、前記数値Ｍは2以上の整数であることを特徴とする、請求項１記載のデータ暗号化装置。

【請求項５】　入力データをＮビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックに対して所定の暗号化処理を施し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力する暗号処理方法であって、

記憶手段が、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶しており、

所定の入力ブロックの暗号処理を行う時は、記憶手段に記憶された連鎖データを所定の初期値に初期化する初期化ステップと、

記憶手段に記憶されている連鎖データを所定の変換で変換し変換データを生成するデータ変換ステップと、

変換データと鍵データを融合して融合データを生成する融合ステップと、

前記所定の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第１部分鍵生成処理を行って部分鍵データを生成し、前記所定の入力ブロック以外の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第２部分鍵生成処理を行って部分鍵データを生成する部分鍵生成ステップと、

部分鍵データに基づいて入力ブロックを暗号化し暗号化データを生成して暗号化ブロックとして出力する暗号化ステップと、

暗号化ステップで生成された暗号化データを新たな連鎖データとして記憶手段に記憶された連鎖データを更新し、次の暗号処理に供させる記憶ステップとを備え、

前記第１部分鍵生成処理と前記第２部分鍵生成処理とは安全性のための処理負荷を異ならせていることを特徴とする暗号処理方法。

【請求項６】　前記第２部分鍵生成処理は、融合データに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって部分鍵生成処理を行い、これにより前記第１部分鍵生成処理よりも安全性のため

の処理負荷を小さくしていることを特徴とする、請求項５記載の暗号処理方法。

【請求項７】　前記データ融合ステップにおけるデータ融合操作は、ビット毎の排他的論理和または加算演算とすることを特徴とする請求項５記載の暗号処理方法。

【請求項８】　前記所定の入力ブロックは、入力されるＭ番目毎の入力ブロックであって、前記数値Ｍは2以上の整数であることを特徴とする請求項５記載の暗号化処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘密鍵に基づいて、被暗号処理データをブロック単位で暗号化する暗号処理装置及び暗号処理方法であって、特に処理速度を大幅に低下させることなく安全性を向上させる技術に関する。

【０００２】

【従来の技術】

近年、ディジタル通信が急速に普及してきたが、健全な産業の発展やプライバシーを保護する等の観点から、通信におけるデータの機密性を確保できる安全性の高いデータ暗号化方式が要求されている。また、暗号化方式に対しては、安全性のみならず暗号処理の高速性及びハードウェア／ソフトウェア両面における実装の簡便性も要求される。

（第１の従来例）

データ暗号化方式の第１の従来例として、擬似乱数加算型暗号がある。

【０００３】

この方式では、送信側・受信側双方が同じ秘密鍵（以下、単に「鍵」という。）を共有しており、平文データＭを一定長の平文データブロックＭｉに区切り、区切られた各Ｍｉに対して、共有している鍵をシードとして平文データブロックＭｉと同じ長さの乱数データＲを発生させる。そして、各平文データブロックＭｉとその乱数データＲとを対応させるビット毎に排他的論理和の計算を行うことによって、暗号文データブロックＣｉを得る。式に表現すると以下の通りである

。

【０００４】

Ｃｉ＝Ｍｉ（＋）Ｒ

ただし、演算子“（＋）”は対応するビット毎の排他的論理和を意味する。

最後に、得られた各暗号文データブロックＣｉを連結し、暗号文Ｃが得られるというものである。

この方式は、暗号化速度が非常に高いという点が特徴であり、画像や音声データのリアルタイム通信におけるデータ暗号化方式として適している。

【０００５】

しかし、この方式は既知平文攻撃に対してきわめて安全性が低い。すなわち、いま暗号化する鍵の値が同じであるとすると、わずか１組の平文データブロックＭｉと暗号文データブロックＣｉを入手しただけで、以下の式より、乱数Ｒが判明するので、他の全ての平文データブロックＭｉを解読することができてしまう。

【０００６】

Ｒ＝Ｍｉ（＋）Ｃｉ

（第２の従来例）

データ撹乱の能力が高い暗号方式としては、ブロック暗号方式というものがある。ブロック暗号方式の具体例としては、ＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ）方式やＦＥＡＬ（ＦａｓｔＤａｔａＥｎｃｉｐｈｅｒｍｅｎｔＡｌｇｏｒｉｔｈｍ）方式といったものがある。

ＤＥＳ方式では、６４ビットの平文ブロックを５６ビットの鍵を用いて暗号化し、６４ビットの暗号文ブロックに変換する。実際の暗号化では、５６ビットの鍵データを元に生成される４８ビット×１６個の部分鍵データを用いる。６４ビット以上の平文に対しては、６４ビットのブロックに分割して、暗号化を行う。ＤＥＳ方式ならびにＦＥＡＬ方式は、岡本栄司著「暗号理論入門」（共立出版）に詳しく述べられている。

（第３の従来例）

第２の従来例であげたブロック暗号方式に対する代表的な解読法として、差分

解読法と線形解読法というものがある。第３の従来例はこれらの解読法に対する安全性を強化する目的で考案された暗号方式である。なお、差分解読法・線形解読法の詳細については、それぞれＥ．Ｂｉｈａｍ，Ａ．Ｓｈａｍｉｒ著，‘‘ＤｉｆｆｅｒｅｎｔｉａｌＣｌｙｐｔｏａｎａｌｙｓｉｓｏｆｔｈｅＤａｔａＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ，’’Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ．及び松井充著，``ＤＥＳ暗号の線形解読法（Ｉ），’’１９９３年暗号と情報セキュリティシンポジウム（ＳＣＩＳ’９３）予稿集ＳＣＩＳ９３－３Ｃ．に記載されている。

【０００７】

差分解読法・線形解読法のいずれにおいても、同一の鍵で暗号化された平文－暗号文ペアを多数用意し、それらを解析することによって暗号化に使用されている鍵を求めるというものである。暗号解読を成功させるためには、同一の鍵データで暗号化された平文－暗号文ペアが多数必要になる。よって、複数の平文ブロックを暗号化する場合に、ブロック毎に異なる鍵データを用いて暗号化を行えば、これらの解読法に対する安全性は強化される。そこで、一つ前の平文ブロックの暗号化から得られる「可変情報」を利用して鍵データを更新していくという方式が考案されている。

【０００８】

ここでは、第３の従来例として特開平１１－７２３９号公報にある鍵連鎖方式を挙げる。この方式では、「可変情報」として１つ前の暗号化で得られる暗号文データを用いて鍵データの更新を行っている。

図６はこの方式のデータ暗号化装置４０の内部構成を示すブロック図である。

データ暗号化部４００は、データ暗号化部４００の外部から入力される１ブロック（６４ビット）の平文データを、部分鍵データ生成部４０１から入力される部分鍵データ３２ビット×１６に従って暗号化し、その結果得られる暗号文データ６４ビットを出力する。

【０００９】

部分鍵データ生成部４０１は、排他的論理和部４０２から入力される入力鍵データ６４ビットをもとに３２ビット×１６の部分鍵データを生成し、データ暗号

化部４００に入力する。

排他的論理和部４０２は、データ暗号化部４００の外部から入力される暗号化鍵データ６４ビットとデータ変換部４０３から入力される６４ビットデータとのビット毎の排他的論理和演算を行い、演算結果を入力鍵データ６４ビットとして出力する。

【００１０】

データ変換部４０３は、レジスタ４０４から入力される６４ビットデータに対して所定の変換操作を行い、結果の６４ビットデータを出力する。

レジスタ４０４は、予め設定された初期値によって初期化されており、１ブロック前の平文の暗号化で得られた６４ビット暗号文データを保管し、次の平文ブロックの暗号化の際に、その保管している６４ビットデータを出力しデータ変換部４０３に入力する。

【００１１】

次に、暗号化する時の動作について述べる。

入力されるデータは６４ビットのブロック単位に先頭からＰ０，Ｐ１，…に分割される。　そしてＰ０から順に６４ビットの平文データとして、データ暗号化装置４０に入力され、６４ビットの暗号化鍵データに従い暗号化される。データ暗号化装置４０では、入力される６４ビットの平文データＰｔ（ｔ＝０，１，…）に対して、以下のような暗号化処理が行われる。

【００１２】

最初に、データ変換部４０３は、レジスタ４０４に保管されている１つ前の暗号文データＣ（ｔ－１）をデータ変換し、その変換された６４ビットデータｆ（Ｃ（ｔ－１））を排他的論理和部４０２に入力する。ただし、ｔ＝０の時には、レジスタ４０４からはレジスタの初期値ＩＶが入力され、その変換データｆ（ＩＶ）を出力する。排他的論理和部４０２はデータ変換部４０３より入力される前記６４ビットデータｆ（Ｃ（ｔ－１））と、前記６４ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の６４ビットデータを入力鍵データとして出力する。

【００１３】

次に部分鍵データ生成部４０１では、排他的論理和部４０２から入力される前記６４ビット入力鍵データを元に３２ビット×１６の部分鍵データを生成し、データ暗号化部４００に入力する。

データ暗号化部４００では、データ暗号化装置４０の外部から入力される６４ビットの平文データＰｔに対して、部分鍵データ生成部４０１から入力される前記６４ビットの部分鍵データ３２ビット×１６に従い、所定の暗号化処理を行ってその結果得られる６４ビットデータをＣｔとする。そして、データ暗号化装置４０はＣｔを出力する。

【００１４】

データ暗号化部４００および部分鍵データ生成部４０１の具体的な処理内容としては、第２の従来例の説明の中で挙げたＤＥＳ暗号方式、ＦＥＡＬ暗号方式、といったブロック暗号方式の暗号化部分および部分鍵生成部分をそれぞれ用いる。

この方式では、６４ビット以上の平文を複数ブロックに分けて暗号化する場合、各平文ブロックの暗号化毎に、入力鍵データが更新される。すなわち、各平文ブロックで異なる入力鍵データを用いて暗号化されるので、解読者は、次のようにして、同一の鍵で暗号化された平文－暗号文のペアを集めるしかない。

【００１５】

すなわち、平文データ系列の先頭ブロックＰ０の暗号化では、同じ入力鍵データ（すなわちｆ（ＩＶ）と鍵データとを排他的論理和演算した値）が部分鍵データ生成部４０１に入力されることが保証できるので、各平文データ系列の先頭ブロックＰ０とそれに対応する暗号文データＣ０を収集することで所要の平文・暗号文ペアを得ることができる。通常、暗号化を行う平文データ系列は、画像・音声データといった膨大なデータ量を有するので、前記の方法で多数の既知平文・暗号文ペアを集めることは、平文の全てのブロックに対して同一の鍵データで暗号化を行う第２の従来例と比べて困難になる。

【００１６】

従って、第３の従来例は、前記の差分解読法・線形解読法といった既知平文攻撃に対する安全性が強化されている。

【００１７】

【発明が解決しようとする課題】

しかしながら、この第３の従来例においては、平文データ１ブロックを暗号化する毎に部分鍵データ生成部４０１は、入力鍵データから部分鍵データを生成する処理を行わなければならず、暗号化の処理速度が低下するという問題がある。

例えば、データ暗号化部４００および部分鍵データ生成部４０１に前述のＦＥＡＬ暗号方式を適用するとする。ＦＥＡＬ暗号方式の部分鍵データ生成部はデータ暗号化部と同程度の処理量を必要とする。通常のＦＥＡＬ暗号方式では、１つの平文データを暗号化する場合に、部分鍵生成は１度行うだけでよいので、画像・音声データなどのデータ長の長い平文データを暗号化する場合には、部分鍵生成処理による速度の低下は無視できるほど小さくなる。

【００１８】

しかし、ＦＥＡＬ暗号方式を第３の従来例に用いて暗号化を行う場合には、ブロック毎に部分鍵生成を実行するので、普通にＦＥＡＬ暗号方式で暗号化を行うよりも暗号化速度が約１／２に低下する。一般に、ブロック暗号方式における鍵生成部はデータ暗号化部と同程度あるいはそれ以上の処理量を必要とするので、上記のような問題はＦＥＡＬ暗号方式の場合に限らず、他のブロック暗号方式についても同様の問題が生じる。

【００１９】

一方、従来例３において部分鍵データ生成部の処理を簡略化すれば暗号化処理速度の低下を小さくすることは可能であるが、その簡略化によって各種解読法、特に既知平文攻撃に対する安全性が低下することになるので、安全性の上で問題である。

そこで、本発明はかかる問題点に鑑みてなされたものであり、鍵更新によって差分解読法・線形解読法といった既知平文攻撃に対する高い安全性を保ちつつ、鍵更新による暗号化処理速度の低下が少ないデータ暗号化装置及び暗号処理方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】

請求項１に係る発明は、入力データをＮビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを前記初期値に初期化するデータ記憶手段と、

前記データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

前記データ変換手段から出力されたデータと前記鍵データを融合するデータ融合手段と、

前記所定の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第１の部分鍵生成処理を行い、前記所定の入力ブロック以外の入力ブロックに対して暗号化を行う時は前記データ融合手段から出力されたデータに基づいて第２の部分鍵生成処理を行う部分鍵生成手段と、

前記部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

前記部分鍵生成手段で行う前記第１の部分鍵生成処理と前記第２の部分鍵生成処理は安全性のための処理負荷を異ならせていることを特徴とする。

【００２１】

請求項２に係る発明は、請求項１の発明において、前記第２の部分鍵生成処理は、前記データ融合手段から出力されたデータに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによって行い、これにより、前記第１の部分鍵生成手段よりも安全性のための処理負荷を小さくしていることを特徴とする。

【００２２】

請求項３に係る発明は、請求項１の発明において、前記データ融合手段におけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする。

請求項４に係る発明は、請求項１の発明において、前記所定の入力ブロックは

、入力されるＭ番目毎の入力ブロックであって、

前記数値Ｍは2以上の整数であることを特徴とする。

【００２３】

請求項５に係る発明は、入力データをＮビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックに対して所定の暗号化処理を施し暗号化ブロックとし、前記暗号化ブロックを連結し暗号文データとして出力する暗号処理方法であって、

記憶手段が、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶しており、

所定の入力ブロックの暗号処理を行う時は、記憶手段に記憶された連鎖データを所定の初期値に初期化する初期化ステップと、

記憶手段に記憶された連鎖データを所定の変換で変換し変換データを生成するデータ変換ステップと、

変換データと鍵データを融合して融合データを生成する融合ステップと、

前記所定の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第１部分鍵生成処理を行って部分鍵データを生成し、前記所定の入力ブロック以外の入力ブロックの暗号処理を行う時は、前記融合データに基づいて第２部分鍵生成処理を行って部分鍵データを生成する部分鍵生成処理ステップと、

部分鍵データに基づいて入力ブロックを暗号化し暗号化データを生成して暗号化ブロックとして出力する暗号化ステップと、

暗号化ステップで生成された暗号化データを新たな連鎖データとして記憶手段に記憶された連鎖データを更新し、次の暗号処理に供させる記憶ステップとを備え、

前記第１部分鍵生成処理と前記第２部分鍵生成処理とは安全性のための処理負荷を異ならせていることを特徴とする特徴とする。

【００２４】

請求項６に係る発明は、請求項５の発明において、前記第２部分鍵生成処理は、融合データに基づいてデータを生成し、前記生成されたデータと同じデータ複数個をビット連結することによってデータを生成を行い、これによって、前記第

１部分鍵生成処理よりも安全性のための処理負荷を小さくしていることを特徴とする。

【００２５】

請求項７に係る発明は、請求項５の発明において、前記データ融合ステップにおけるデータ融合操作は、ビット毎の排他的論理和、または加算演算とすることを特徴とする。

請求項８に係る発明は、請求項５の発明において、前記所定の入力ブロックは、入力されるＭ番目毎の入力ブロックであって、前記数値Ｍは2以上の整数であることを特徴とする。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

通常、データ暗号化装置で暗号化された暗号文データは、暗号化した際の鍵データを、共有しているデータ復号化装置で暗号化変換と逆変換となる演算を施され、平文データとなって出力される。本実施形態では、データ暗号化装置を有する送信機において、ある平文データが暗号化されて暗号文データとなって送信され、その暗号文データがデータ復号化装置を有する受信機で復号化されて平文データとなり出力されるという暗号通信システムとして説明する。

（暗号通信システムの構成）

図１は、本実施形態に係る暗号通信システムの構成を示すブロック図である。

【００２７】

この暗号通信システムは、送信機１および受信機２から構成される。

送信機１は、図１に示されるように、データ暗号化装置１０及び送信部１１を備える。データ暗号化装置１０には、６４ビットの平文データと６４ビットの暗号化鍵データが入力される。この平文データは、ディジタル符号化された音声または画像情報をはじめとするディジタル情報である。また、暗号化鍵データは、予め送信機１と受信機２との間で定めていたものである。これら平文データと鍵データは、データ暗号化装置１０に入力され処理を施されて６４ビットの暗号文データとなる。一般に、暗号化の対象となる平文データは６４ビット以上のデー

タであることが多い。その場合は、平文データを６４ビット単位に分割して順次データ暗号化装置１０に入力して暗号化していく。そして、送信部１１により並列ｔｏ直列変換、変調及び増幅され伝送路３を経て受信機２に送信される。

【００２８】

受信機２は、図１に示されるように、データ復号化装置２０及び受信部２１を備える。データ復号化装置２０には、受信部２１を介して受信され６４ビット毎に直列ｔｏ並列変換された暗号文データが入力されていく。また、予め送信機１と受信機２で定めている６４ビットの暗号化鍵データが入力されている。入力される６４ビット暗号文データは、データ復号化装置２０で暗号化鍵データに従って処理を施されて復号文データとなる。

（データ暗号化装置１０の構成）

図２は、図１に示されるデータ暗号化装置１０の構成を示すブロック図である。

【００２９】

本図において、このデータ暗号化装置１０は、データ暗号化部１００と部分鍵データ生成部１０１と、排他的論理和部１０２と、データ変換部１０３と、レジスタ１０４と、カウンター１０５と、部分鍵データ生成制御部１０６と、レジスタ制御部１０７とを備えている。

部分鍵データ生成部１０１は、予め定められた所定周期Ｔに対してＴ×ｎ（ｎ＝０，１，．．．）ブロック目の平文を暗号化するときに限り、処理量が通常よりも多い（処理負荷の大きい）部分鍵生成処理を行い、レジスタ１０４は、Ｔ×ｎ（ｎ＝０，１，．．．）ブロック目の平文を暗号化するときに限り、レジスタの内容を予め設定されている初期値ＩＶで初期化することを特徴とする。なお、本実施例では、所定の周期Ｔを２＾１０とする。ここで“α＾β”はαをβ乗した値を表す。

【００３０】

以下では、各部の処理内容について説明する。

データ暗号化部１００は、６４ビット毎に分割されて入力される平文データを、部分鍵データ生成部１０１から入力される３２ビット×１６の部分鍵データを

用いて暗号化し、６４ビット暗号文データを出力する。

部分鍵データ生成部１０１は、部分鍵データ生成制御部１０６から入力される制御信号に従って２つの異なる部分鍵生成処理のうちから１つを選択し、排他的論理和部１０２より入力される６４ビットの入力鍵データに対して、選択された部分鍵データ生成処理を行い、３２ビット×１６の部分鍵データを生成し、出力する。

【００３１】

排他的論理和部１０２は、データ暗号化装置１０の外部から入力される６４ビットの暗号化鍵データとデータ変換部１０３から入力される６４ビットデータとのビット毎の排他的論理和演算を行い、演算結果の６４ビットデータを入力鍵データとして出力する。

データ変換部１０３は、レジスタ１０４から入力される６４ビットデータに対して所定のデータ変換処理を行い、変換結果の６４ビットデータを出力する。尚、本実施例では所定のデータ変換処理を、上位方向への１３ビットローテートシフトとする。

【００３２】

レジスタ１０４は、内部に保管している６４ビットデータをデータ変換部１０３に入力する。また、保管データは予め設定されている初期値ＩＶで初期化されており、データ暗号化部１００から６４ビット暗号文データの入力があった場合には、保管データをその入力データに更新する。さらに、レジスタ制御部１０７から制御信号“１”の入力があった場合に限り、保管データを初期値ＩＶに初期化する。

【００３３】

カウンター１０５は、内部に保管するカウント値が初期値０で初期化されているものとし、データ暗号化部１００が６４ビット平文データの暗号化処理を実行し、６４ビット暗号文データを出力する度にカウント値を１だけ増加させて更新する。但し、カウント値（２＾１０－１）は０に更新されるものとする。

部分鍵データ生成制御部１０６は、カウンター１０５のカウント値が０のときには、部分鍵データ生成部１０１に制御信号“１”を入力し、０以外のときには

制御信号“０”を入力する。

【００３４】

レジスタ制御部１０７は、カウンター１０５のカウント値が０のときには、レジスタ１０４に制御信号“１”を入力し、レジスタ１０４を初期値ＩＶで初期化させる。カウント値が０以外のときには、制御信号“０”を入力する。

次に、暗号化する時の動作について述べる。

入力される平文データは６４ビットのブロック単位に先頭からＰ０，Ｐ１，…に分割される。そしてＰ０から順に６４ビットの平文データとして、データ暗号化装置１０に入力され、６４ビットの暗号化鍵データに従い暗号化される。データ暗号化装置１０では、入力される６４ビットの平文データＰｔ（ｔ＝０，１，…）に対して、以下のような暗号化処理が行われる。

【００３５】

暗号化の前に、カウンター１０５のカウント値は初期値０に設定され、レジスタ１０４の保管データは初期値ＩＶに設定されているとする。

まず、部分鍵データ生成制御部１０６およびレジスタ制御部１０７は、カウンター１０５のカウント値が０のときには、制御信号“１”を部分鍵データ生成部１０１およびレジスタ１０４にそれぞれ入力し、カウント値が０以外のときには、制御信号“０”を部分鍵データ生成部１０１およびレジスタ１０４にそれぞれ入力する。

【００３６】

次に、レジスタ１０４は、レジスタ制御部１０７から制御信号“１”が入力されたときに限り、保管データを初期値ＩＶに初期化し、制御信号“０”が入力されたときには、初期化は行わない。その後、レジスタ１０４は、内部に保管している６４ビットデータをデータ変換部１０３に入力する。

次に、データ変換部１０３はレジスタ１０４から入力される６４ビットデータをデータ変換し、その変換された６４ビットデータを排他的論理和部１０２に入力する。その後、排他的論理和部１０２はデータ変換部１０３より入力される６４ビットデータと、６４ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の６４ビットデータを入力鍵データとして部分鍵データ生成部１０１に

入力する。

【００３７】

次に部分鍵データ生成部１０１は、排他的論理和部１０２から入力される６４ビット入力鍵データに対して、部分鍵データ生成制御部１０６から入力される制御信号に従って選択した部分鍵データ生成処理によって３２ビット×１６の部分鍵データを生成し、生成された部分鍵データをデータ暗号化部１００に入力する。

【００３８】

その後、データ暗号化部１００は、データ暗号化装置１０の外部から入力される６４ビットの平文データＰｔに対して、部分鍵データ生成部１０１から入力される６４ビットの部分鍵データ３２ビット×１６に従って暗号化を行い、その結果の６４ビット暗号文データをＣｔとする。そして、データ暗号化装置１０はＣｔを出力する。カウンター１０５は、データ暗号化部１００が1ブロックの平文データを暗号化して、６４ビットの暗号文データを出力する度に、内部のカウント値を１だけ増加させて更新する。但し、カウント値（２＾１０－１）は０に更新されるものとする。

【００３９】

そして、レジスタ１０４は、保管データをデータ暗号化部１００から出力される前記６４ビット暗号文データＣｔに更新する。

以上の操作を繰り返し行い、暗号化処理を行う。

尚、データ暗号化部１００としては、従来例２で述べたＦＥＡＬ暗号方式のデータ暗号化部分を用いるものとする。

（データ復号化装置２０の構成）

図３は、図１に示されるデータ復号化装置２０の構成を示すブロック図である。

【００４０】

本図において、このデータ復号化装置２０は、データ復号化部２００と部分鍵データ生成部２０１と、排他的論理和部２０２と、データ変換部２０３と、レジ

スタ２０４と、カウンター２０５と、部分鍵データ生成制御部２０６と、レジスタ制御部２０７とを備えている。

部分鍵データ生成部２０１は、予め定められた所定周期Ｔに対してＴ×ｎ（ｎ＝０，１，．．．）ブロック目の暗号文を復号化するときに限り、処理量が通常よりも多い（処理負荷の大きい）部分鍵生成処理を行い、レジスタ２０４は、Ｔ×ｎ（ｎ＝０，１，．．．）ブロック目の暗号文を復号化するときに限り、レジスタの内容を予め設定されている初期値ＩＶで初期化することを特徴とする。なお、本実施例では、所定の周期Ｔを２＾１０とする。

【００４１】

データ復号化部２００は、６４ビット毎に分割されて入力される暗号文データを、部分鍵データ生成部２０１から入力される３２ビット×１６の部分鍵データを用いて復号化し、６４ビット平文データを出力する。

部分鍵データ生成部２０１は、部分鍵データ生成制御部２０６から入力される制御信号に従って２つの異なる部分鍵生成処理のうちから１つを選択し、排他的論理和部２０２より入力される６４ビットの入力鍵データに対して部分鍵データ生成処理を行い、３２ビット×１６の部分鍵データを生成し、出力する。

【００４２】

排他的論理和部２０２は、データ復号化装置２０の外部から入力される６４ビットの暗号化鍵データとデータ変換部２０３から入力される６４ビットデータとのビット毎の排他的論理和演算を行い、演算結果の６４ビットデータを入力鍵データとして出力する。

データ変換部２０３は、レジスタ２０４から入力される６４ビットデータに対して、所定のデータ変換処理を行い、変換結果の６４ビットデータを出力する。尚、本実施例では所定のデータ変換処理を、上位方向への１３ビットローテートシフトとする。

【００４３】

レジスタ２０４は、内部に保管している６４ビットデータをデータ変換部２０３に入力する。また、保管データは予め設定されている初期値ＩＶで初期化されており、一つ前のブロックの復号化の時に入力された６４ビット暗号文データを

保管している。但し、レジスタ制御部２０７から制御信号“１”が入力された場合に限り、保管データを初期値ＩＶに初期化する。

【００４４】

カウンター２０５は、内部に保管するカウント値が初期値０で初期化されているものとし、データ復号化部２００が６４ビット暗号文データの復号化処理を実行し、６４ビット平文データを出力する度にカウント値を１だけ増加させて更新する。但し、カウント値（２＾１０－１）は、０に更新されるものとする。

部分鍵データ生成制御部２０６は、カウンター２０５のカウント値が０のときには、部分鍵データ生成部２０１に制御信号“１”を入力し、０以外のときには制御信号“０”を入力する。

【００４５】

レジスタ制御部２０７は、カウンター２０５のカウント値が０のときには、レジスタ２０４に制御信号“１”を入力し、カウント値が０以外のときには、制御信号“０”を入力する。

次に、復号化する時の動作について述べる。

入力される暗号文データは６４ビットのブロック単位に先頭からＣ０，Ｃ１，…に分割される。そしてＣ０から順に６４ビットの暗号文データとして、データ復号化装置２０に入力され、６４ビットの暗号化鍵データに従い復号化される。データ復号化装置２０では、入力される６４ビットの暗号文データＣｔ（ｔ＝０，１，…）に対して、以下のような復号化処理が行われる。

【００４６】

復号化の前に、カウンター２０５のカウント値は初期値０に設定され、レジスタ２０４の保管データは初期値ＩＶに設定されているとする。

まず、部分鍵データ生成制御部２０６およびレジスタ制御部２０７は、カウンター２０５のカウント値が０のときには、制御信号“１”を部分鍵データ生成部２０１およびレジスタ２０４にそれぞれ入力し、カウント値が０以外のときには、制御信号“０”を部分鍵データ生成部２０１およびレジスタ２０４にそれぞれ入力する。

【００４７】

次に、レジスタ２０４は、レジスタ制御部２０７から制御信号“１”が入力されたときに限り、保管データを初期値ＩＶに初期化し、制御信号“０”が入力されたときには、初期化は行わない。その後、レジスタ２０４は、内部に保管している６４ビットデータをデータ変換部２０３に入力する。

次に、データ変換部２０３はレジスタ２０４から入力される６４ビットデータをデータ変換し、その変換された６４ビットデータを排他的論理和部２０２に入力する。その後、排他的論理和部２０２は、データ変換部２０３より入力される６４ビットデータと、６４ビットの暗号化鍵データとの排他的論理和演算を行い、その結果の６４ビットデータを入力鍵として部分鍵データ生成部２０１に入力する。

【００４８】

次に部分鍵データ生成部２０１は、排他的論理和部２０２から入力される６４ビットの入力鍵データに対して、部分鍵データ生成制御部２０６から入力される制御信号に従って選択した部分鍵生成処理によって、３２ビット×１６の部分鍵データを生成し、生成した部分鍵データをデータ復号化部２００に入力する。

その後、データ復号化部２００は、データ復号化装置２０の外部から入力される６４ビットの暗号文データＣｔに対して、部分鍵データ生成部２０１から入力される６４ビットの部分鍵データ３２ビット×１６に従って復号化を行い、その結果の６４ビット平文データをＰｔとする。そして、データ復号化装置２０はＰｔを出力する。

【００４９】

カウンター２０５は、データ復号化部２００が1ブロックの暗号文データを復号化して、６４ビットの平文データを出力する度に、内部のカウント値を１だけ増加させて更新する。但し、カウンター値（２＾１０－１）は０に更新されるものとする。

そして、データ復号化部２００でのデータ復号化処理が終わり、平文データが出力された後に、レジスタ２０４は、保管データを前記６４ビット暗号文データＣｔに更新する。

【００５０】

以上の操作を繰り返し行い、復号化処理を行う。

尚、データ復号化部２００には、ＦＥＡＬ暗号化方式のデータ復号化部を用いるものとする。

（部分鍵データ生成部１０１，２０１の構成）

図４は、図２，図３に示す部分鍵データ生成部１０１，２０１の構成の一例を示すブロック図である。尚、部分鍵データ生成部１０１，２０１は全く同じ構成をとる。

【００５１】

本図において、この部分鍵データ生成部１０１，２０１は、データ乱数化部３０１と、乱数化データ保管部３０２と、段数制御部３０３とを備えている。

データ乱数化部３０１は、段数制御部３０３から入力される６４ビットに対して、所定のデータ乱数化処理を行い、３２ビット部分鍵データＳＫおよび６４ビット乱数化データを出力する。尚、３２ビット部分鍵データＳＫは乱数化データ保管部３０２に入力され、６４ビット乱数化データは段数制御部３０３に入力される。

【００５２】

段数制御部３０３は、データ乱数化部３０１が合計で何回データ乱数化処理を行ったかを制御する。データ乱数化処理の合計回数が所定の回数に満たない場合、段数制御部３０３は、データ乱数化部３０１が出力する６４ビット乱数化データを再びデータ乱数化部３０１に入力し、データ乱数化操作を繰り返し行わせる。但し、データ乱数化部３０１が１回目のデータ乱数化処理を行うときには、部分鍵データ生成部３００の外部から入力される６４ビット入力鍵をデータ乱数化部３０１に入力する。また、所定の回数は、制御信号“１”が入力された場合には、１６回とし、制御信号“０”が入力された場合には、２回とする。

【００５３】

乱数化データ保管部３０２は、データ乱数化部３０１から入力される３２ビット部分鍵データを保管し、データ乱数化部３０１が所定回数のデータ乱数化処理を実行した後、３２ビット×１６の部分鍵データを出力する。乱数化データ保管部３０２は、入力される制御信号によって、以下に示すように異なった処理を行

う。

【００５４】

制御信号“１”が入力された場合、乱数化データ保管部３０２は、データ乱数化部３０１から最初に入力される３２ビット部分鍵データをＳＫ０、２番目に入力される３２ビット部分鍵データをＳＫ１、…、１６番目に入力される３２ビット部分鍵データをＳＫ１５として保管し、データ乱数化部３０１が１６回のデータ乱数化処理を終えた後、保管している３２ビット×１６の部分鍵データＳＫ０，…，ＳＫ１５を出力する。

【００５５】

制御信号“０”が入力された場合、乱数化データ保管部３０２は、データ乱数化部３０１から最初に入力される３２ビット部分鍵データをＳＫ０、２番目に入力される３２ビット部分鍵データをＳＫ１として保管する。データ乱数化部３０１が２回のデータ乱数化処理を終えた後、ＳＫ１４＝ＳＫ１２＝ＳＫ１０＝ＳＫ８＝ＳＫ６＝ＳＫ４＝ＳＫ２＝ＳＫ０、および、ＳＫ１５＝ＳＫ１３＝ＳＫ１１＝ＳＫ９＝ＳＫ７＝ＳＫ５＝ＳＫ３＝ＳＫ１とした３２ビット×１６の部分鍵データＳＫ０，…，ＳＫ１５を出力する。

（データ乱数化部３０１の構成）

図５は、図４に示すデータ乱数化部３０１の構成の一例を示すブロック図である。

【００５６】

本図において、このデータ乱数化部３０１は、データ撹乱部３０１０と、排他的論理和部３０１１とを備えている。

データ撹乱部３０１０は、３２ビットの入力データに対して、データ乱数化部３０１の外部から入力される６４ビットデータの上位３２ビットデータに基づいてデータ撹乱操作を行い、その結果の３２ビット撹乱データを出力する。

【００５７】

排他的論理和部３０１１は、データ乱数化部３０１の外部から入力される６４ビットデータの上位３２ビットデータとデータ撹乱部３０１０から入力される３２ビットデータとのビット毎の排他的論理和演算を行い、その演算結果の３２ビ

ットデータを出力する。

データ乱数化部３０１の動作を以下で説明する。

データ乱数化部３０１の外部から入力される６４ビットデータは、まず最初に、上位３２ビットをＡ１、下位３２ビットをＡ０として、２つの３２ビットデータＡ１，Ａ０に分割される。そして、Ａ１は排他的論理和部３０１１およびデータ撹乱部３０１０に入力され、Ａ０はデータ撹乱部３０１０に入力されると同時に、そのまま３２ビットデータＢ１として出力される。データ撹乱部３０１０は、３２ビットデータＡ０を３２ビットデータＡ１に基づいてデータ撹乱し、結果の３２ビット撹乱データを出力する。

【００５８】

次に、排他的論理和部３０１１は、３２ビット撹乱データと３２ビットデータＡ１とのビット毎の排他的論理和演算を行い、演算結果を３２ビットデータＢ０として出力すると同時に３２ビット部分鍵データとしても出力する。

以上の操作で得られた３２ビットデータＢ１，Ｂ０について、Ｂ１を上位３２ビット、Ｂ０を下位３２ビットとしてビット連結した６４ビットデータを、データ乱数化部３０１の出力データとして出力する。

【００５９】

尚、データ撹乱部３０１０には、第２の従来例で述べたＦＥＡＬ暗号方式のデータ撹乱部を用いるものとする。

（暗号通信システムの動作）

次に、上述の図１～図５を参照し、本暗号通信システム全体の動作を説明する。

【００６０】

送信機１においては、入力されたデータは６４ビット単位に先頭からＰ０，Ｐ１，Ｐ２，…に平文データとして分割される。そして、Ｐ０から順にデータ暗号化装置１０に入力されて、送信機１に予め保持されている６４ビットの暗号化鍵データに従って、暗号化される。暗号化処理は（２＾１０）×ｋブロック目の平文データの暗号化処理だけが、他の平文ブロックの処理とは異なることを特徴する。但し、ｋ＝０，１，…とする。具体的には、データ暗号化装置１０では、入

力される平文データＰｔ（ｔ＝０，１，…）に対して、以下のような暗号化処理が行われる。

【００６１】

レジスタ１０４は、レジスタ制御部１０７の制御の下で、ｔ個目のデータＰｔを暗号化するときには、以下に示す６４ビットデータＲ０ｔを出力する。

Ｒ０ｔ＝Ｃ（ｔ－１）（ｔ≠（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式１）

Ｒ０ｔ＝ＩＶ（ｔ＝（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式２）

次に、データ変換部１０３は、レジスタ１０４からの入力に対してデータ変換処理を行い、以下に示す６４ビットデータＳ０ｔを出力する。

【００６２】

Ｓ０ｔ＝ｆ（Ｒ０ｔ）　……（式３）

但し、ｆ（Ｘ）は入力データＸに対して、データ変換部１０３でのデータ変換処理を行った結果の値を表す。

次に、排他的論理和部１０２は、データ変換部１０３からの入力に対して、以下に示す６４ビットデータＩＫ０ｔを出力する。

【００６３】

ＩＫ０ｔ＝Ｓ０ｔ（＋）ＥＫ　……（式４）

但し、ＥＫはデータ暗号化装置１０の外部から入力される、暗号化鍵データであり、“（＋）”はビット毎の排他的論理和演算を表す。

次に、部分鍵データ生成部１０１は、部分鍵データ生成制御部１０６の制御の下で、排他的論理和部１０２からの入力に対して、以下に示す、３２ビット×１６の部分鍵データＳＫ０ｔを出力する。

【００６４】

ＳＫ０ｔ＝ＫＧＡ（ＩＫ０ｔ）（ｔ≠（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式５）

ＳＫ０ｔ＝ＫＧＢ（ＩＫ０ｔ）（ｔ＝（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式６）

ＫＧＡ（Ｘ）は、入力データＸに対して、部分鍵データ生成制御部１０６から制御信号“０”が入力された場合の部分鍵データ生成処理を行った結果の値を表し、ＫＧＢ（Ｘ）は制御信号“１”が入力された場合の部分鍵データ生成処理を行った結果の値を表す。

【００６５】

次に、データ暗号化部１００は、部分鍵データ生成部１０１からの入力及びデータ暗号化装置１０の外部から入力される平文データＰｔに対して、以下に示す暗号文データＣｔを出力する。

Ｃｔ＝Ｅｎｃ（Ｐｔ，ＳＫ０ｔ）　……（式７）

送信部１１では、Ｃ０，Ｃ１，…を先頭から連結して暗号文データとして受信機２に送信する。

【００６６】

受信機２においては、入力されたデータは６４ビット単位に先頭からＣ０，Ｃ１，Ｃ２，…の順に暗号文データとして分割される。そして、Ｃ０から順にデータ復号化装置２０に入力されて、受信機２に予め保持されている６４ビットの暗号化鍵データを用いて、復号化される。

データ復号化装置２０では、入力される暗号文データＣｔ（ｔ＝０，１，…）に対して、以下のような復号化処理が行われる。

レジスタ２０４は、レジスタ制御部２０７の制御の下で、ｔ個目のデータＥｔを復号化するときには、以下に示す６４ビットデータＲ１ｔを出力する。

【００６７】

Ｒ１ｔ＝Ｃ（ｔ－１）（ｔ≠（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式８）

Ｒ１ｔ＝ＩＶ（ｔ＝（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式９）

次に、データ変換部２０３は、レジスタ２０４からの入力に対してデータ変換処理を行い、以下に示す６４ビットデータＳ１ｔを出力する。

【００６８】

Ｓ１ｔ＝ｆ（Ｒ１ｔ）　……（式１０）

但し、ｆ（Ｘ）は入力データＸに対して、データ変換部２０３でのデータ変換処理を行った結果の値を表す。

次に、排他的論理和部２０２は、データ変換部２０３からの入力に対して、以下に示す６４ビットデータＩＫ１ｔを出力する。

【００６９】

ＩＫ１ｔ＝Ｓ１ｔ（＋）ＥＫ　……（式１１）

但し、ＥＫはデータ復号化装置２０の外部から入力される、暗号化鍵データであり、“（＋）”はビット毎の排他的論理和演算を表す。

次に、部分鍵データ生成部２０１は、部分鍵データ生成制御部２０６の制御の下で、排他的論理和部２０２からの入力に対して、以下に示す３２ビット×１６の部分鍵データＳＫ１ｔを出力する。

【００７０】

ＳＫ１ｔ＝ＫＧＡ（ＩＫ１ｔ）（ｔ≠（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式１２）

ＳＫ１ｔ＝ＫＧＢ（ＩＫ１ｔ）（ｔ＝（２＾１０）×ｋ，ｋ＝０，１，…の場合）　……（式１３）

ＫＧＡ（Ｘ）は、入力データＸに対して、部分鍵データ生成制御部２０６から制御信号“０”が入力された場合の部分鍵データ生成処理を行った結果の値を表し、ＫＧＢ（Ｘ）は制御信号“１”が入力された場合の部分鍵データ生成処理を行った結果の値を表す。

【００７１】

次に、データ復号化部２００は、部分鍵データ生成部２０１からの入力及びデータ復号化装置２０の外部から入力される暗号文データＥｔに対して、以下に示す復号文データＤｔを出力する。

Ｄｔ＝Ｄｅｃ（Ｃｔ，ＳＫ１ｔ）　……（式１４）

平文データ列Ｐ０，Ｐ１，…に対して、６４ビットの暗号化鍵データを用いて暗号化した暗号文データ列Ｃ０，Ｃ１，…を同じ６４ビットの暗号化鍵データを用いてデータ復号化装置２０で復号した復号文データＤ０，Ｄ１，…は、平文データＰ０，Ｐ１，…に等しい。次にそのことを示す。

【００７２】

（式１），（式２）及び（式８），（式９）より、

Ｒ０ｔ＝Ｒ１ｔ　（ｔ＝０，１，…）　……（式１５）

が成り立つ。この（式１５）と（式３），（式１０）から、

Ｓ０ｔ＝Ｓ１ｔ　（ｔ＝０，１，…）　……（式１６）

が成り立つ。次に、この（式１６）と（式４），（式１１）とから、

ＩＫ０ｔ＝ＩＫ１ｔ　（ｔ＝０，１，…）　……（式１７）

が成り立つ。よって、この（式１７）および（式５），（式６），（式１２），（式１３）から

ＳＫ０ｔ＝ＳＫ１ｔ　（ｔ＝０，１，…）　……（式１８）

が成り立つ。ここで、（式７），（式１４）から、

Ｄｔ＝Ｄｅｃ（Ｅｎｃ（Ｐｔ，ＳＫ０ｔ），ＳＫ１ｔ）　（ｔ＝０，１，…）

……（式１９）

が成り立つが、Ｅｎｃ，Ｄｅｃについては、任意の６４ビットデータα，βについて、以下のような関係式（式２０）が成り立つ

α＝Ｄｅｃ（Ｅｎｃ（α，β），β）　……（式２０）

よって、（式１９），（式２０）及び（式１８）から、

Ｄｔ＝Ｐｔ

が成り立つことがいえる。

【００７３】

次に本データ暗号化装置１０の安全性及について述べる。本データ暗号化装置１０の安全性はデータ暗号化部１０１の安全性に大きく依存している。本実施形態の場合、データ暗号化部１０１へ入力される入力鍵データＩＫ０ｔは、各６４ビットの平文データＰｔの暗号化毎に更新していくので、第３の従来例と同様、入力鍵データを全て同じとする第２の従来例と比べて安全性が向上している。

ｔ≠（２＾１０）×ｋ（ｋ＝０，１，…）なる平文ブロックＰｔの暗号化では、データ暗号化部１００に入力される３２ビット×１６の部分鍵データＳＫ０，…，ＳＫ１５については、ＳＫ０＝ＳＫ２＝…＝ＳＫ１４及びＳＫ１＝ＳＫ３＝…＝ＳＫ１５であることから、ＳＫ０，ＳＫ１，…，ＳＫ１５の値がすべて異なる

場合と比べて既知平文攻撃に対する安全性は弱くなる。しかし、それらの平文ブロックの暗号化で用いられる入力鍵データＩＫ０ｔは、

ＩＫ０ｔ＝ＥＫ（＋）Ｃ（ｔ－１）

となり、その中で同じＩＫ０ｔを用いて暗号化されている平文ブロックを大量に収集することは、Ｃ（ｔ－１）が２＾６４通り（ここでα＾βはαをβ乗した値を表す）の値を取りうることからほとんど不可能に近いといえる。よって、この方法による既知平文攻撃は成功しない。

【００７４】

一方、ｔ＝（２＾１０）×ｋ（ｋ＝０，１，…）なる平文ブロックＰｔの暗号化では、データ暗号化部１００に入力される３２ビット×１６の部分鍵データＳＫ０，…，ＳＫ１５は、全て異なる値となるように生成されるので、この方法による既知平文攻撃の安全性は、第３の従来例と全く同じになる。

次に本データ暗号化装置１０の暗号化処理速度性能について述べる。

ｔ≠（２＾１０）×ｋ（ｋ＝０，１，…）なる平文ブロックＰｔの暗号化では、部分鍵データ生成部１０１は、実質は３２ビット×２の部分鍵データを生成しているのと同じである簡便な処理によって部分鍵生成データ３２ビット×１６を生成しているので、各ブロック毎に部分鍵データを生成することによる、暗号化処理速度の低下は、第３の従来例よりも少なくて済む。

【００７５】

なお、本実施形態においては、データ変換部１０３，２０３の６４ビット出力データと、暗号化鍵データとの融合手段として、ビット毎の排他的論理和演算を用いているが、これはビット毎の排他的論理和でなくても、同様な効果が得られる。

また、本実施形態においては、データ変換部１０３，２０３から出力される変換データは６４ビットとしているが、これは６４ビットである必要はない。例えば、暗号化鍵データが５６ビットである場合には、出力データが５６ビットとなるようなデータ変換部を用いれば良い。

【００７６】

また、本実施形態においては、レジスタ１０４，２０４に１つ前の暗号化で生

成される暗号文データを入力しているが、これは１つ前の暗号化の処理過程で得られる６４ビットの値であれば何でもよい。さらにこの値は、６４ビットである必要はなく、６４ビット以下、例えば４０ビットといった場合には、入力データが４０ビットとなるようなデータ変換手段を、データ変換部１０３，２０３に用いればよい。

【００７７】

また、本実施形態においては、データ暗号化部１００としてＦＥＡＬ暗号方式を用いているが、これはブロック暗号方式であれば何でもよい。

また、部分鍵データ生成部１０１は、本実施形態に用いた構成に限定されるものではなく、６４ビットの入力鍵データから、３２ビット×１６の部分鍵データを生成するものであればよい。

【００７８】

また、部分鍵データ生成部１０１で用いる異なる2種類の暗号化処理は、本実施形態に用いた様な乱数化の処理量を異ならせる構成に限定されるものではなく、制御信号“１”が入力された時に選択される暗号化処理が、制御信号“０”が入力された時に選択される暗号化処理よりも処理負荷の大きいものであれば何でもよい。

【００７９】

また、カウンター１０５，２０５はカウント値（２＾１０－１）を０に更新するものとしているが、これは、（２＾１０－１）という値に制限されるものではなく、任意の正の整数であれば何でもよいし、０への更新を行わなくてもよい。

また、本実施形態では、６４ビットの暗号化鍵データを装置内に保管しているが、これは最初の暗号化に用いる６４ビットの暗号化鍵データだけを最初に保管しておき、残りの暗号化鍵データは暗号化されて平文データと共に伝送するようにするか、実鍵データを更新する度に、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式などの公開鍵暗号方式を用いて、暗号化鍵データを配送し、共有するようにしてもよい。

【００８０】

【発明の効果】

以上の説明から明らかなように、本発明は、入力データをＮビット単位の入力ブロックに分割し、予め与えられた鍵データに基づいて、順次前記入力ブロックを所定のアルゴリズムに従って暗号化し暗号化ブロックとし、暗号化ブロックを連結し暗号文データとして出力するデータ暗号化装置であって、

予め初期データが設定されていて、ある入力ブロックに先立ってデータ出力された暗号化ブロックを記憶し、予め設定されている所定の入力ブロックに対して暗号化を行うときには記憶データを初期値に初期化するデータ記憶手段と、

データ記憶手段の記憶データを所定の変換で変換するデータ変換手段と、

データ変換手段から出力されたデータと鍵データを融合するデータ融合手段と、

所定の入力ブロックに対して暗号化を行う時はデータ融合手段から出力されたデータに基づいて第１の部分鍵生成処理を行い、所定の入力ブロック以外の入力ブロックに対して暗号化を行う時はデータ融合手段から出力されたデータに基づいて第２の部分鍵生成処理を行う部分鍵生成手段と、

部分鍵生成手段から出力されたデータに基づいて入力ブロックを暗号化して暗号化ブロックとして出力するデータ暗号化手段とを備え、

部分鍵生成手段で行う第１の部分鍵生成処理と第２の部分鍵生成処理は安全性のための処理負荷を異ならせているため、従来の様に全ての入力ブロックに対して安全性のための処理負荷の大きい部分鍵生成を行うのではなく、ある特定の入力ブロックに対してのみ安全性のための処理負荷の大きい部分鍵生成を行い、これにより、処理速度の低下を少なくして、暗号の安全性を高めることが可能である。

【００８１】

よって、本発明によれば従来と同様の安全性向上の効果を得ながらも、従来よりも高速な暗号処理を実現するものであり、特にマルチメディア技術の進展が望まれる今日における画像情報等のリアルタイム秘密通信等に好適であり、その実用効果は極めて大きい。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る暗号通信システムの構成を示すブロック図

【図２】

同データ暗号化装置１０の構成を示すブロック図

【図３】

同データ復号化装置２０の構成を示すブロック図

【図４】

同部分鍵データ生成部１０１，２０１の構成を示すブロック図

【図５】

同データ乱数化部３０１の構成を示すブロック図

【図６】

従来のデータ暗号化装置の構成を示すブロック図

【符号の説明】

１　　送信機

２　　受信機

３　　伝送路

１０　　データ暗号化装置

１１　　送信部

２０　　データ復号化装置

２１　　受信部

１００　データ暗号化部

１０１　部分鍵データ生成部

１０２　排他的論理和部

１０３　データ変換部

１０４　レジスタ

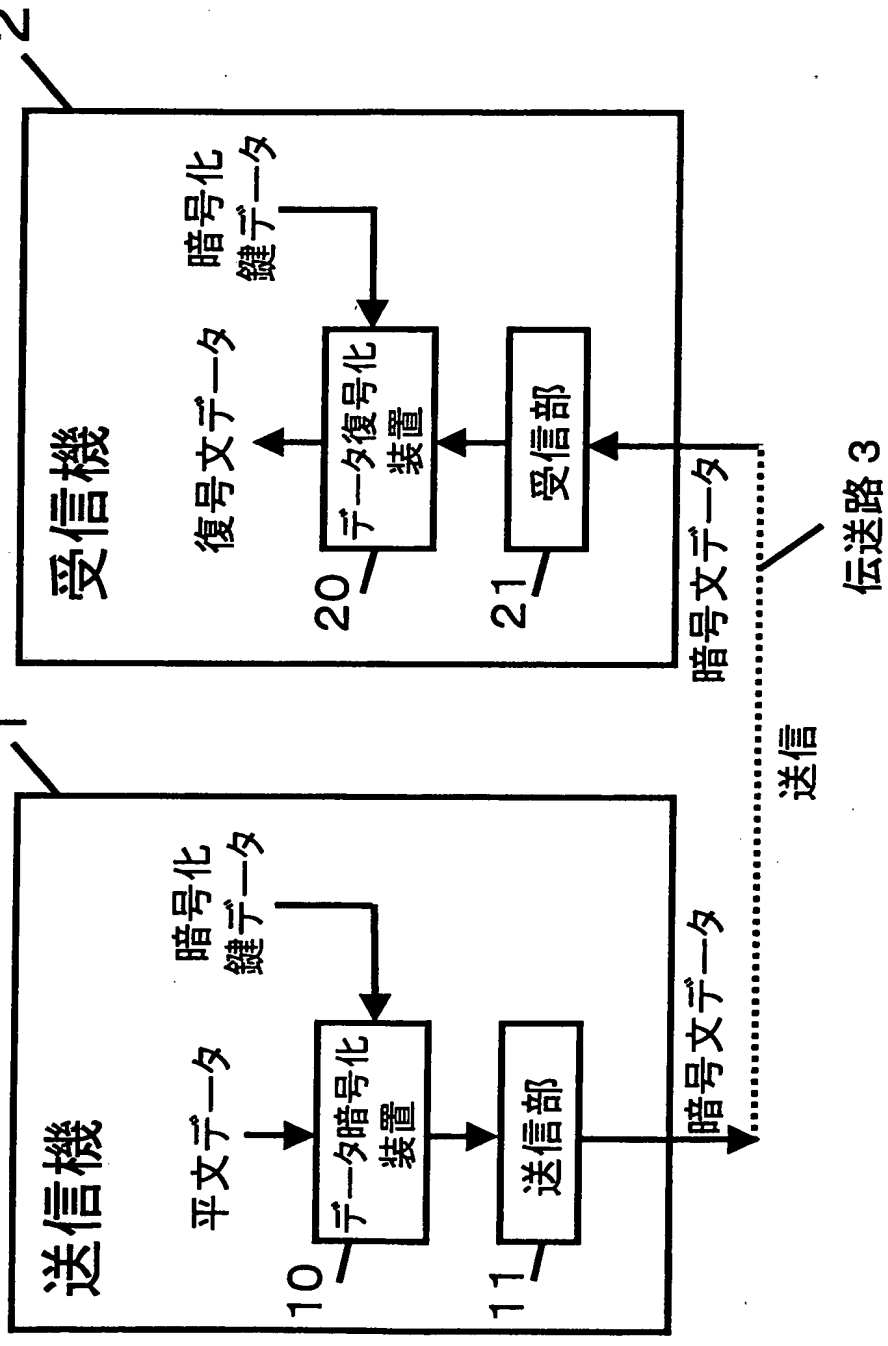
１０５　カウンター

１０６　部分鍵データ生成制御部

１０７　レジスタ制御部

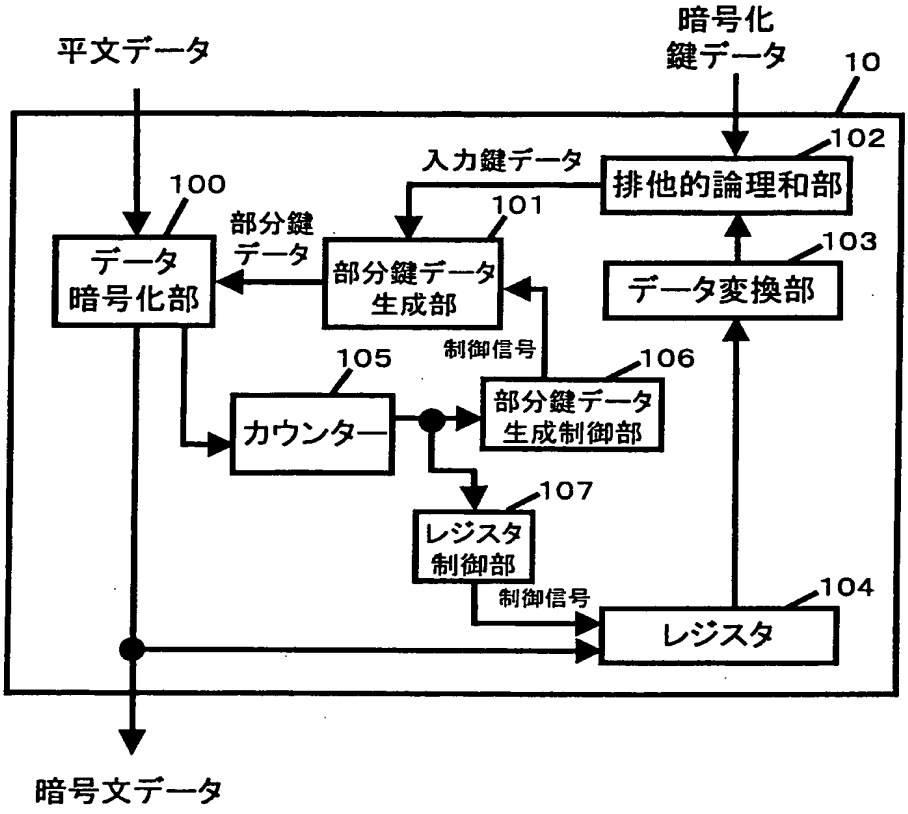
【書類名】　図面

【図１】



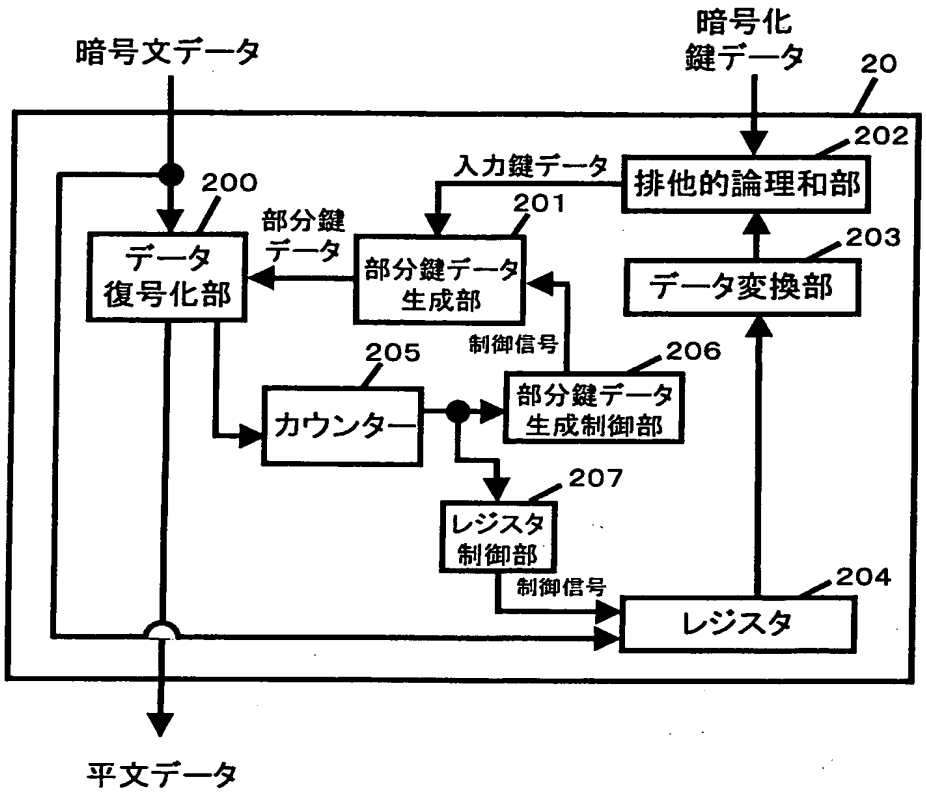
出証特２０００－３０４３２７６

【図２】

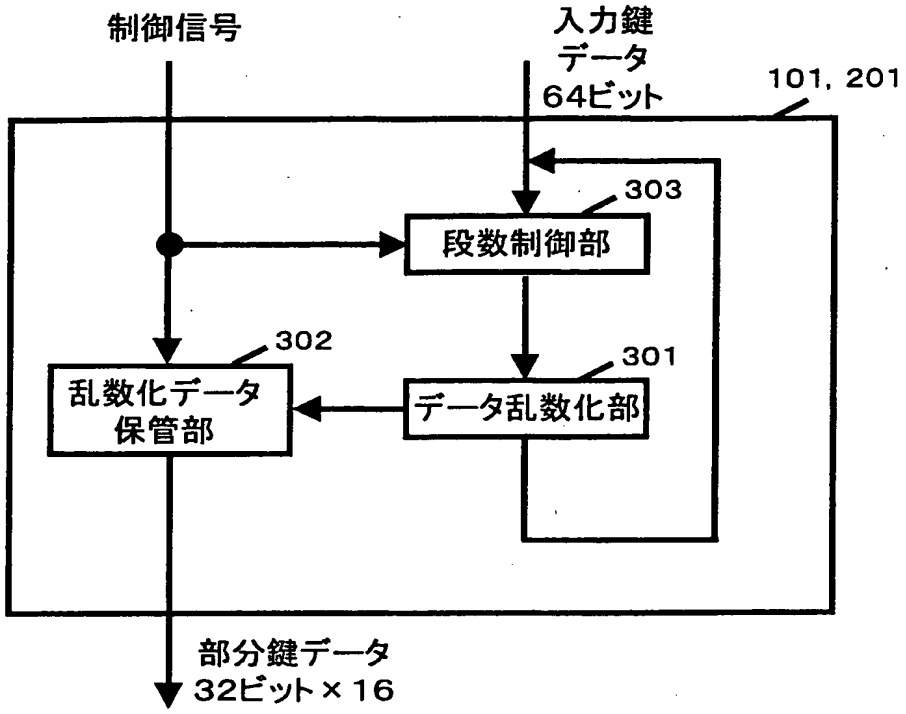


出証特２０００－３０４３２７６

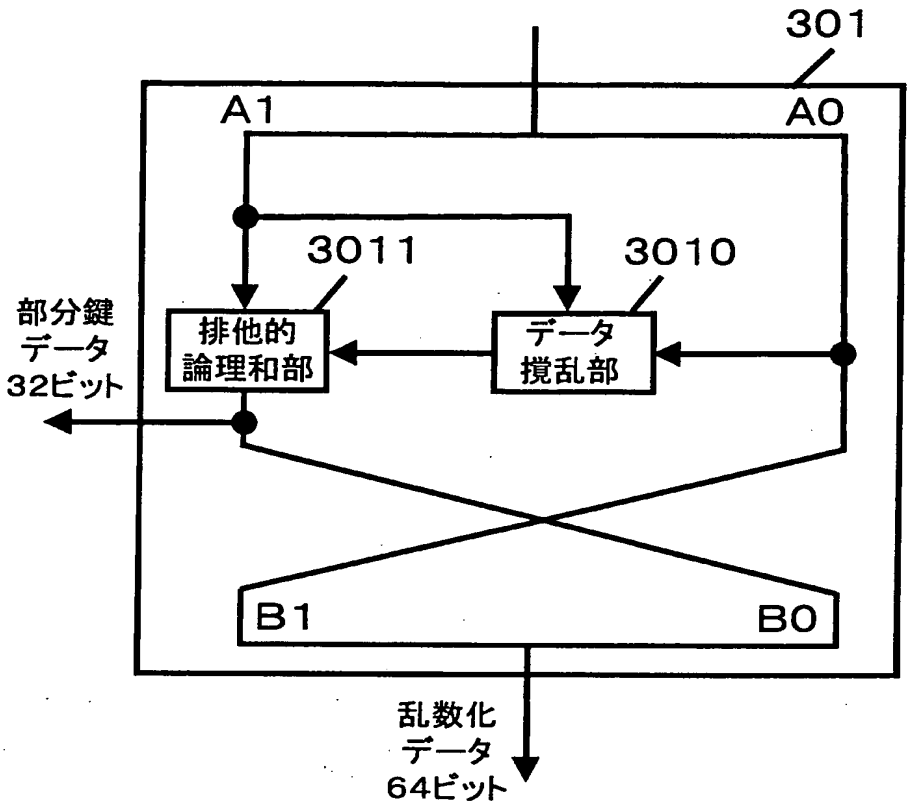
【図３】


暗号文データ
暗号化
鍵データ
20
202
入力鍵データ
排他的論理和部
200
201
部分鍵
データ
データ
復号化部
部分鍵データ
生成部
203
データ変換部
制御信号
205
206
カウンター
部分鍵データ
生成制御部
207
レジスタ
制御部
制御信号
204
レジスタ
平文データ

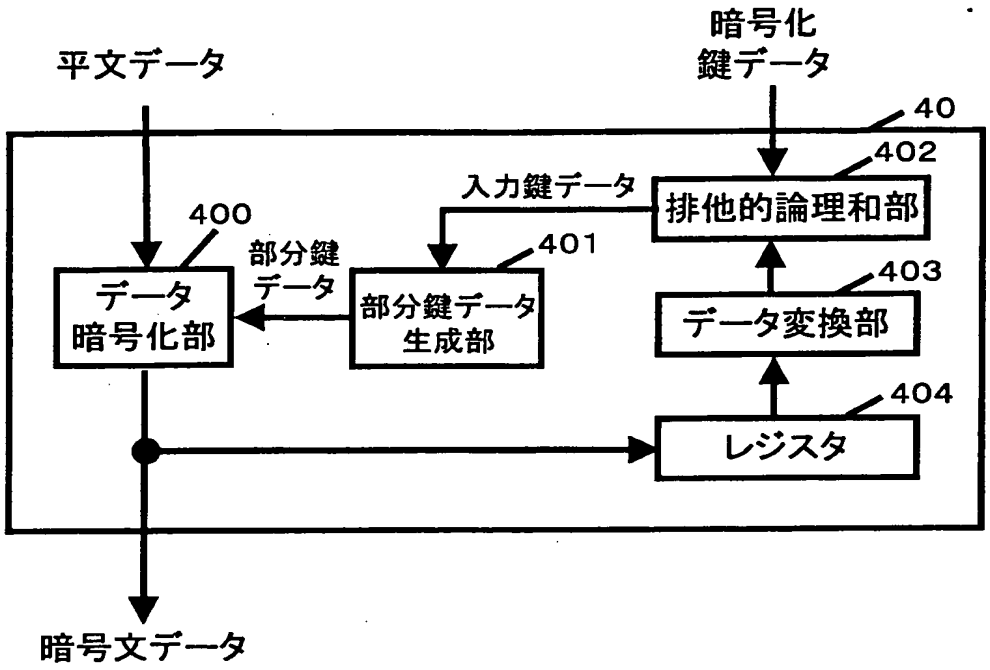
【図４】


制御信号
入力鍵
データ
64ビット
101, 201
303
段数制御部
302
乱数化データ
保管部
301
データ乱数化部
部分鍵データ
32ビット×16

【図５】


301
A1
A0
3011
3010
部分鍵
データ
32ビット
排他的
論理和部
データ
撹乱部
B1
B0
乱数化
データ
64ビット

【図６】


暗号化
鍵データ
平文データ
40
402
入力鍵データ
排他的論理和部
400
部分鍵
データ
401
403
データ
暗号化部
部分鍵データ
生成部
データ変換部
404
レジスタ
暗号文データ

【書類名】　要約書

【要約】

【課題】　直前の平文ブロックから得られる可変情報を用いて鍵データを更新していく暗号方式は、安全性の向上が実現できる一方、１ブロック暗号化を行う毎に部分鍵生成を行うことから、処理速度が大幅に低下する。

【解決手段】　特定の平文ブロックの暗号化には、安全性のための処理負荷の大きい部分鍵生成処理を行い、それ以外の平文ブロックの暗号化には、処理負荷の小さい部分鍵生成処理を行うことで、処理速度低下が少なく、安全性の向上したデータ暗号化装置、暗号処理方法を実現する。

【選択図】　図2

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　神奈川県川崎市幸区堀川町７２番地
氏　名　　株式会社東芝